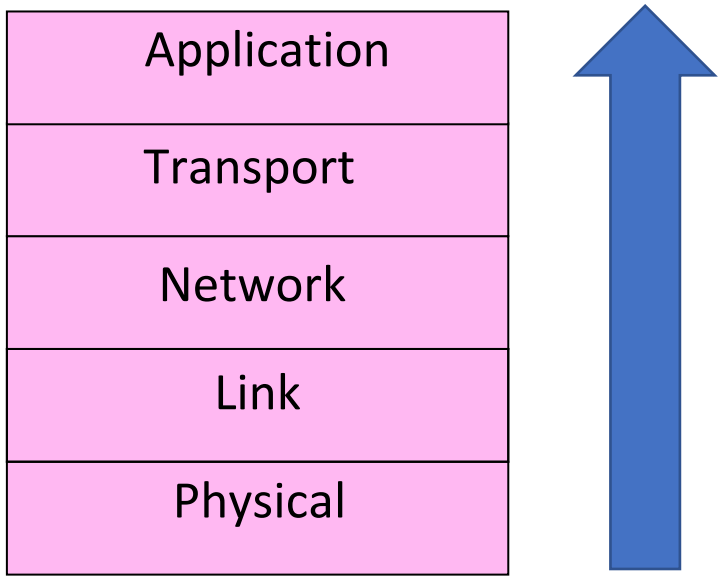
Network Security

Where we are

- Security crosses all layers



Security Threats

- "Security" is like "performance"
  - Means many things to many people
  - Must define the properties we want

- Key task is clearly stating the threat model
  - The dangers and attacker's abilities
  - Can't assess risk or solution effectiveness otherwise

Security Threats (2)

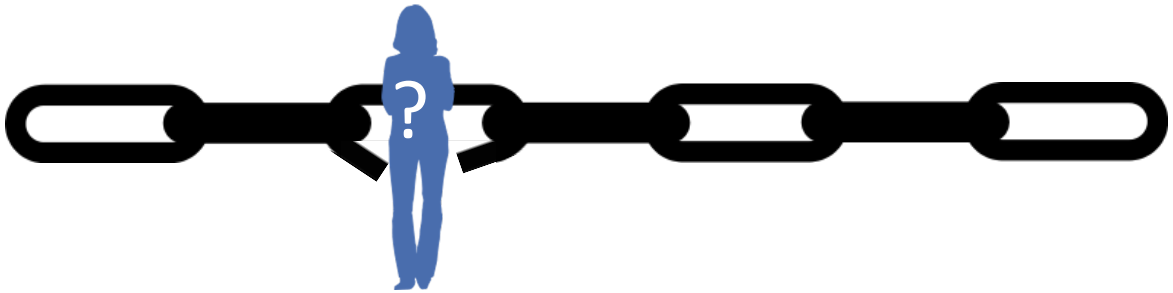
- Some example threats
  - It's not all about encrypting messages

Attacker	Ability	Threat
Eavesdropper	Intercept messages	Read contents of message
Observer	Inspect packet destinations	Collect conversations
Intruder	Compromised host	Tamper with contents of message
Impersonator	Remote social engineering	Trick party into giving information
Extortionist	Remote / botnet	Disrupt network services

Risk Management

- Security is hard as a negative goal
  - Try to ensure security and don't let anything bad happen!

- Only as secure as the weakest link
  - Could be design flaw or bug in code
  - But often the weak link is elsewhere …



Risk Management (2)

- 802.11 security … early on, WEP:
  - Cryptography was flawed; can run cracking software to read WiFi traffic
- Today, WPA2/802.11i security:
  - Computationally infeasible to break!
- So that means 802.11 is secure against eavesdropping?

Risk Management (3)

- Many possible threats
  - We just made the first one harder!
  - 802.11 is more secure against eavesdropping in that the risk of successful attack is lower. But it is not “secure”.

Threat Model	Old WiFi (WEP)	New WiFi (WPA2)
Break encryption from outside	Very easy	Very difficult
Guess WiFi password	Often possible	Often possible
Get password from computer	May be possible	May be possible
Physically break into home	Difficult	Difficult

Cryptography

Cryptology

- Rich history, especially spies / military
  - From the Greek “hidden writing”
- Cryptography
  - Focus is encrypting information
- Cryptanalysis
  - Focus is how to break codes
- Modern emphasis is on codes that are “computationally infeasible” to break
  - Takes too long compute solution

Uses of Cryptography

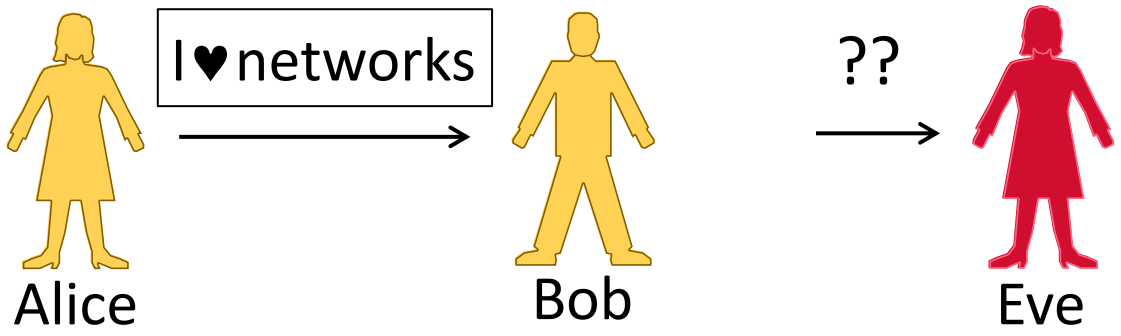
- Encrypting information is useful for more than deterring eavesdroppers (confidentiality)
  - Prove message came from real sender (authentication)
  - Prove remote party is who they say
  - Prove message hasn’t been altered (integrity)
- Designing secure cryptographic scheme tricky!
  - Use approved design (library) in approved way
  - And even then ….. OpenSSL earlier this year

Internet Reality

- Most of the protocols were developed before the Internet grew popular
  - It was a smaller, more trusted world
  - So protocols lacked security …
- We have strong security needs today
  - Clients talk with unverified servers
  - Servers talk with anonymous clients
  - Security has been retrofitted
  - This is far from ideal!

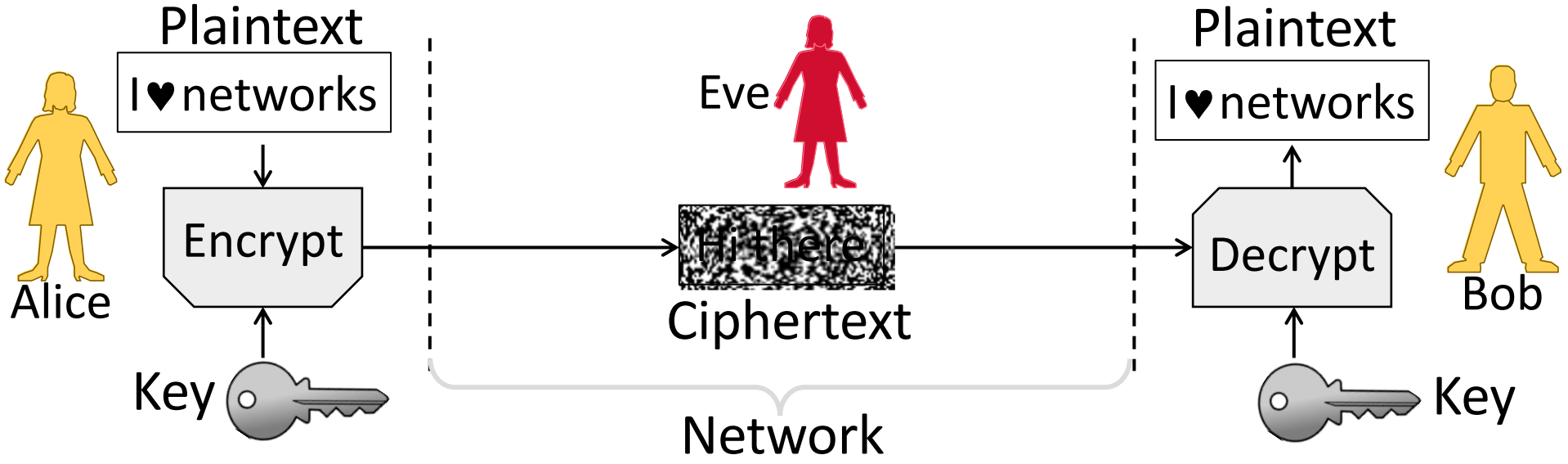
Confidentiality: Goal, Threat Model

- Goal: Send a private message from Alice to Bob
- Threat: Eve will read the message
  - Eve is a passive adversary (observer)



Encryption/Decryption Model

- Alice encrypts private message (plaintext) using key
- Eve sees ciphertext but not plaintext
- Bob decrypts using key to get the private message



Encryption/Decryption (2)

- Encryption is a reversible mapping
  - Ciphertext is encrypted plaintext
- Assume attacker knows algorithm
  - Security does not rely on its secrecy
- Algorithm is parameterized by keys
  - Security does rely on key secrecy
  - Must be distributed (Achilles' heel)

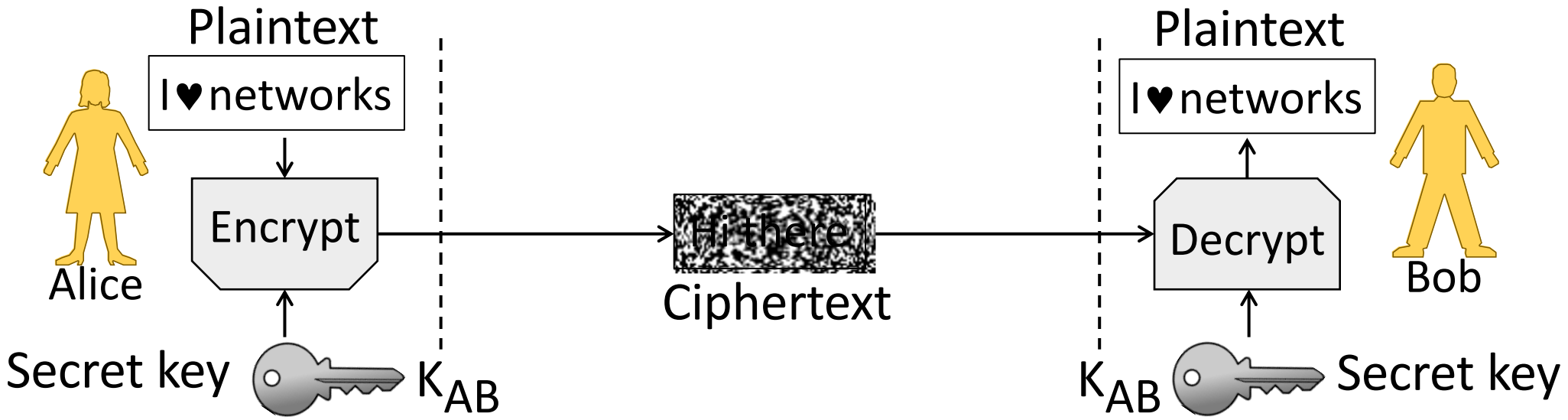
Encryption/Decryption (3)

Two main kinds of encryption:

1. Symmetric key encryption », e.g., AES
   - Alice and Bob share secret key
   - Encryption is a bit mangling box
2. Public key encryption », e.g., RSA
   - Alice and Bob each have a key in two parts: a public part (widely known), and a private part (only owner knows)
   - Encryption is based on mathematics (e.g., RSA is based on difficulty of factoring)

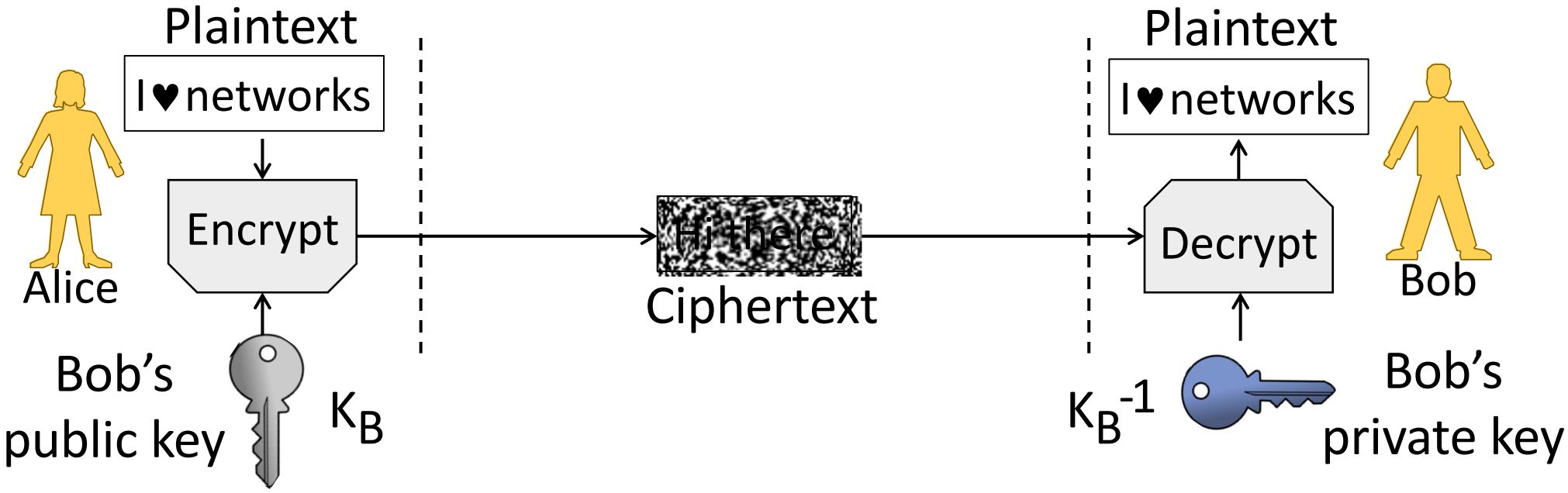
Symmetric (Secret Key) Encryption

- Alice and Bob have the same secret key, K_{AB}
  - Anyone with the secret key can encrypt/decrypt



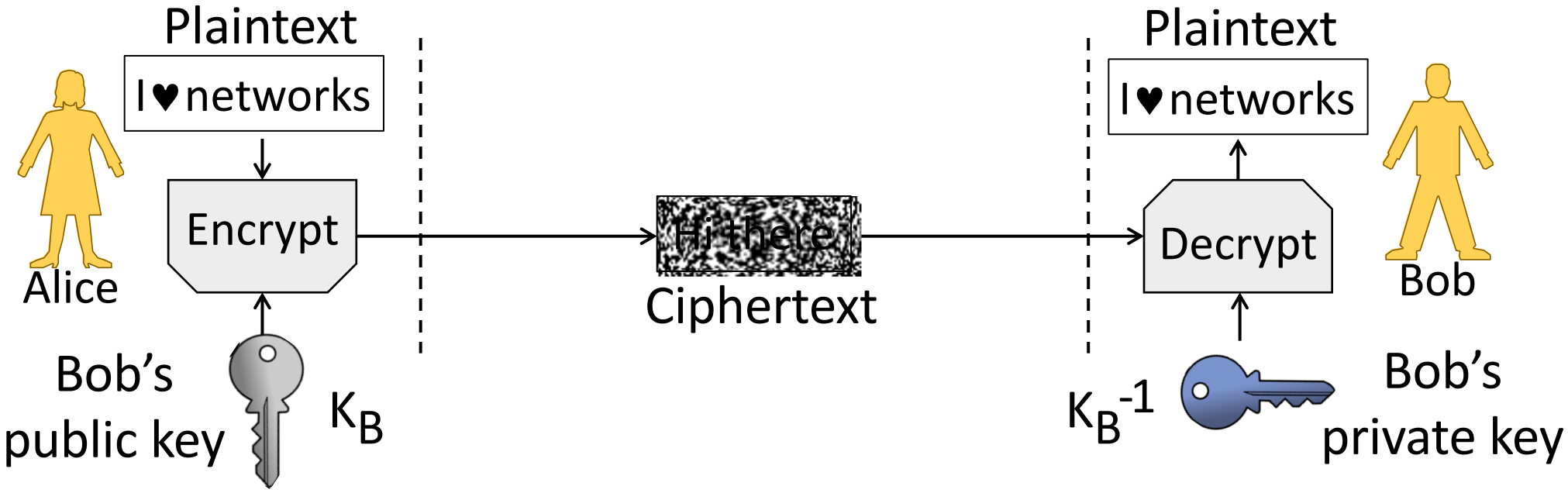
Public Key (Asymmetric) Encryption

- Alice and Bob have public/private key pairs (K_B / K_B^{-1})
  - Public keys are well-known, private keys are secret

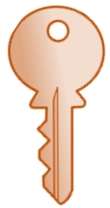


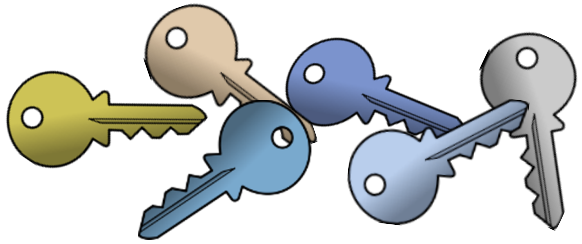
Public Key Encryption (2)

- Alice encrypts w/ Bob's pubkey K_B; anyone can send
- Bob decrypts w/ his private key K_B^{-1}; only he can



Key Distribution





- This is a big problem on a network!
  - Often want to talk to new parties
- Symmetric encryption problematic
  - Have to first set up shared secret
- Public key idea has own difficulties
  - Need trusted directory service
  - We'll look at certificates later

Symmetric vs. Public Key

- Have complementary properties
  - Want the best of both!

Property	Symmetric	Public Key
Key Distribution	Hard – share secret per pair of users	Easier – publish public key per user
Runtime Performance	Fast – good for high data rate	Slow – few, small, messages

Winning Combination

- Alice uses public key encryption to send Bob a small private message
  - It's a key! (Say 256 bits.)
- Alice/Bob send messages with symmetric encryption
  - Using the key they now share
- The key is called a session key
  - Generated for short-term use